chapter 1

5G 시대의 차세대 IoT 보안

최동진 ‖ LG유플러스 책임

2G와 3G 가입자 수는 줄고 있지만 전체 이동통신 가입자 수는 빠르게 증가하고 있다. 2019년 서비스를 개시한 5G 이동통신은 4G 대비 약 10배 이상의 성능 향상이 기대된다. 5G는 타산업과 융합된 4차 산업혁명의 핵심 인프라로서, 신규 서비스 출현, 통신 기기의 다양화, 기기간 연결 급증 등 통신환경의 변화를 초래할 것이며, 이에 따라 5G를 대표하는 AICBM(Aritficial Intelligence, IoT, Cloud, Big Data, Mobile) 중에서도 IoT 영역에 대해 5G 시대에 적합한 보안 방안을 마련하는 것이 시급한 상황이다. 2019년 7월에 정부는 혁신성장동력 특별위원회를 발족시키고 여러 규제를 완화하여 다양한 IoT 제품과 서비스가 가능한 환경이 되었다. 국내외 여러 기관 및 단체에서 상이한 유형의 IoT 보안 가이드를 제시하고 있다. 본 고에서는 다양한 가이드들과 침해 사례를 고찰하고 이에 대한 보안·예방 대책을 제시하고자 한다.

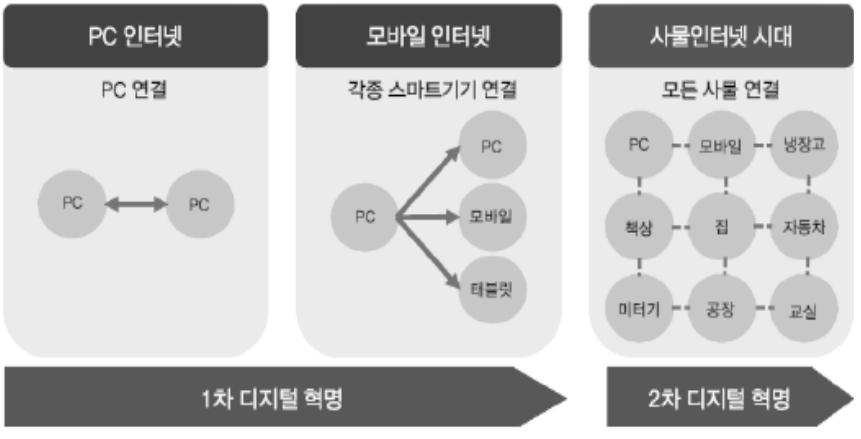
I. 서론

18세기 후반 영국의 증기기관 등장으로 1차 산업혁명이, 19세기 후반에서 20세기 초에는 전기 에너지 발명으로 2차 산업혁명이, 20세기 후반에는 컴퓨터와 인터넷의 등장으로 3차 산업혁명이 발생했다. 그 후 얼마 되지 않아서 직관에 의한 기계의 방대한 데이터 반복 학습에 의해 4차 산업혁명이 발생했다. 4차 산업혁명은 AICBM 즉, 인공지능(Artificial

* 본 내용은 최동진 책임(☎ 010-8080-3603, super301@naver.com)에게 문의하시기 바랍니다.
** 본 내용은 필자의 주관적인 의견이며 IITP의 공식적인 입장이 아님을 밝힙니다.

Intelligence), 사물인터넷(Internet of Things), 클라우드(Cloud), 빅데이터(Big Data) 그리고 모바일(Mobile)의 통합된 서비스 형태로 나타난다. 이를 AICBM 플랫폼 서비스라 하며 농업, 의료, 보안, 자동차 등 거의 모든 분야에서 플랫폼 서비스로 나타날 것이다. 2019년 가트너 전략 기술 트렌드의 10개 항목 중, Smart Spaces, Digital Twins, Empowered Edge, Autonomous Things 등은 모두 직간접적으로 IoT와 관련을 맺고 있지만 이외에도 Augmented Analytics나 인공지능 주도 개발 또한 IoT와 관련이 있다. 그리고 디지털 윤리와 개인정보보호 또한 IoT와 밀접한 관계를 가지고 있다. 따라서, IoT의 도입 시에 가장 큰 문제점일 수 있는 보안의 중요성이 더욱 부각되고 있다.

IoT 보안에 대한 대비는 아직도 많이 부족하지만 IoT 보안에 대한 지출은 늘고 있다. 그러나 IoT 보안에 대한 낮은 인지 수준으로 인해 전략적으로 보안 정책을 수립하고 이에 따라 보안 아키텍처를 구현하기보다는 임시방편으로 제품이나 서비스를 선택함으로써 보안에 여전히 취약하다. 구체적이고 엄격한 규정의 부재는 미흡한 보안 상황을 야기하므로 규제의 준수가 IoT 보안에서 가장 중요한 요소이다. IoT 보안을 위해서는 디바이스 관리, 연결 관리, 애플리케이션 관리, 리포팅 및 분석에 이르는 IoT 관리 플랫폼이 필요하나 아직 IoT의 보안 구성요소에 대한 기술표준이나 규격이 없으므로 이에 대한 대비를 정부나 표준화기관 등이 수행하여야 하며 IoT 보안을 제도화해야 할 것이다. 1차 디지털혁명을 넘어 2차 디지털혁명으로 가는 사물인터넷의 진화는 [그림 1]과 같다[1].



〈자료〉 강남희, "사물인터넷 보안을 위한 표준기술 동향", 한국통신학회지(정보와통신) 31.9, 2014, pp.40-45.

[그림 1] 사물인터넷(IoT)의 진화

II. 5G에서의 IoT 보안 영역

5G는 4차 산업혁명의 핵심 인프라로서 타산업과 융합되어 신규 서비스 출현, 통신 기기의 다양화, 기기간 연결 급증 등 통신환경의 변화를 초래할 것으로 예상된다. 이러한 변화 속에서 5G 시대에 대응하기 위해 IoT 보안이 시급한 상황이다. 5G 이동통신은 3GPP에서 논의가 시작되어 ITU에서 IMT-2020이라는 공식 명칭을 채택하였다. 모든 서비스를 단일 네트워크에서 구현하고자 기술을 개발 중이며 향후 차세대 네트워크는 5G를 중심으로 전개될 전망이다. 과기정통부는 2015년의 미래성장동력특별위원회 기능을 확대, 조정하여 혁신성장동력 특별위원회를 2019년 7월 출범시키고 범정부 차원의 컨트롤타워 역할을 재정비하였다.

5G는 망 구축 및 운용의 효율성을 높이고 유연한 네트워크 구조로 단일 네트워크에서 다양한 서비스가 가능하다. 기존 이동통신의 장점을 계승함과 동시에 신규 개발 기술 및 서비스를 수용할 수 있도록 하였다. 기존 LTE와의 호환성과 LTE-Advanced Pro 표준화도 포함하여 기존 네트워크와의 연동으로 상·하위 호환성을 확보하고 있다. 제공 서비스의 종류(예; 모바일 브로드밴드, 사물인터넷 등), 이용 주파수 대역 등에 따라 자원을 효율적으로 활용하도록 설계되었다. 1개 캐리어 내에서 15kHz폭 부반송파 간격의 numerology로 초고속 광대역 통신을 지원하는 동시에, 60kHz폭 부반송파 간격의 numerology로 다지점 협력 통신(CoMP)을 사용하여 공장 자동화와 같은 산업용 사물 인터넷 애플리케이션이나 실시간 반응 속도가 요구되는 서비스를 위한 초고신뢰·저지연 통신의 지원이 가능하다. 하나의 물리적 네트워크 상에서 논리적으로 네트워크를 분리함으로써, 구축된 네트워크 인프라를 보다 유연하고 효율적으로 운용할 수 있다[11],[14]. 1개의 물리적 네트워크를 이동통신, 자율주행자동차, 사물인터넷 등 여러 개의 논리적 네트워크 슬라이스로 분리하여 각각의 서비스를 제공한다. 물리적 자원을 상황에 따라 유연하게 활용하기 위해 여러 하드웨어들을 소프트웨어 기반으로 운영·관리하는 구조를 가지고 있다.

기타 5G 핵심 기술로는 클라우드 코어를 통한 트래픽 분산 및 초저지연 통신 처리, TDD 주파수의 유연한 상·하향 대역폭을 활용하여 더 많은 안테나로 네트워크 용량과 커버리지를 모두 향상시키고 산란파를 고집적 빔으로 변환하는 대량 다중 입력 다중 출력 및 빔 포밍(Beam Forming) 기술 등이 있다. IoT는 기본적으로 인터넷 기반이므로 모든 제품이 해킹의 대상이 될 수 있다. IoT 디바이스는 종류와 기능이 다양하고 최소한의 프로

[표 1] IoT 유형별 주요 보안 위협

유형	주요 제품	주요 보안 위협	주요 보안 위협 원인
멀티미디어	스마트 TV, 스마트 냉장고 등	PC 환경에서의 모든 악용 행위 카메라/마이크 내장 시 사생활 침해	인증 매카니즘 부재 강도가 약한 비밀번호 펌 업데이트 취약점 물리적 보안 취약점
생활가전	청소기, 인공지능 로봇 등	알려진 운영체제 취약점 및 인터넷 기반 해킹 위협 로봇 청소기에 내장된 카메라에 의한 사생활 침해	인증 매카니즘 부재 펌 업데이트 취약점 물리적 보안 취약점
네트워크	홈캠, 네트워크 카메라 등	무선신호 교란, 정보유출, 데이터 위변조, 서비스 거부 사진 및 동영상의 외부 유출로 사생활 침해	접근통제 부재 전송 데이터 보호 부재 물리적 보안 취약점
제어	디지털 도어락, 가스밸브 등	제어기능 탈취로 도어락 임의 개폐	인증 매카니즘 부재 강도가 약한 비밀번호 접근 통제 부재 물리적 보안 취약점
	모바일 앱(웹) 등	앱(웹) 소스코드 노출로 IoT 기능 탈취	인증정보 평문 저장 전송 데이터 보호 부재
센서	온/습도 센서 등	잘못된 또는 위변조된 온/습도 정보 전송	전송 데이터 보호 부재 데이터 무결성 부재 물리적 보안 취약점

〈가전〉 한국인터넷진흥원, 홈·가전 IoT 보안가이드, 2017. 7.

세싱 성능과 메모리로 운영해야 하므로 보안 솔루션 탑재가 어려운 경우가 많다. 또한, 관심과 수요는 증가하고 있으나 보안 의식이 낮아 기존보다 다양한 보안 위협이 존재하고 있다. [표 1]은 한국인터넷진흥원에서 발표한 IoT 유형별 주요 제품에 대한 주요 보안 위협과 그 원인을 보여주고 있다[8],[19],[20],[22],[23].

한국인터넷진흥원(KISA)에서 IoT 취약점 신고포상제를 시행하고 있는데, 지속적으로 신고 건수가 늘어나고 있다. 자동화된 공격 툴로 디바이스에 접속을 시도하여 전력량, 영상정보의 탈취와 IP 카메라 해킹 등과 같은 IoT 취약점을 공격한 사례들은 다음과 같다[3],[6],[13],[29].

첫째, '인세캠(Insecam)'은 전세계 약 7만 3,000여 대의 IP 카메라를 해킹하여 생중계하였고 한국도 약 6,000여개의 IP 카메라가 해킹되었다. 해커는 출고 당시 기본 설정을 바꾸지 않은 IP 카메라를 해킹하고 위도와 경도를 알 수 있는 구글 지도도 이용하여 가정이나 사무실 등 여러 곳의 영상정보를 탈취하였다. IoT 취약점이 발견된 이후 패치가 이루어졌어도 이용자가 해당 패치를 업데이트하지 않아 무방비 상태로 노출되는 경우도 많이

있다. 이 감염된 IoT 디바이스는 분산 서비스 거부(Distributed Denial of Service: DDoS) 공격에 악용되기도 한다.

둘째, 공격자가 IoT 디바이스들의 알려진 취약점과 기본 패스워드 설정을 악용하여 악성코드 '미라이(Mirai)'로 IoT 기기를 탈취한 뒤 DNS 호스팅 업체 딘(Dyn)을 DOS 공격하여 딘이 관리하던 트위터, 넷플릭스, 페이팔과 주요 언론사 등 유명 웹사이트들이 마비되었다. 추가적으로 미라이 악성코드 개발자가 소스코드를 공개하여 변종 악성코드가 계속해서 발생되고 있다. 이렇듯, 해킹 수법은 점차 지능적으로 고도화되고 있다.

셋째, 한국인터넷진흥원 접수 사례로, 공격자가 취약한 공유기 비밀번호를 악용, 대량으로 해킹하여 스마트폰 앱을 감염시켜 탈취 정보로 포털사이트 계정들을 부정하게 생성하였다. 랜섬웨어가 개인 PC나 회사 서버를 포함하여 스마트 기기 등을 감염시키면 그 피해 규모와 범위는 상당히 크다.

넷째, 사회기반시설에 대해서는 일리노이주 수처리시스템, Duqu, Night Dragon, Nitro,

[표 2] IoT 분야별 보안 위협 시나리오

분야	보안 취약성 및 공격 유형
CCTV	CCTV에 탑재된 카메라 해킹, 사생활 영상 추출
스마트 가전	로봇청소기 취약점 해킹, 탑재된 카메라로 실시간 영상 유출
홈	홈 IoT를 해킹, 도어락 해킹, 전력량 해킹, 가스락 해킹, 물 누수, 전등 해킹
공장	기계 오작동, 전력량 해킹, 물 누수, 관제 해킹(CCTV 등)
공유기	공유키 해킹, 악성코드를 넣어 DDoS 공격 창구로 활용
교통	도로차량 감지기술 내 결함, 센서를 가장해 교통관리 시스템에 위변조 데이터 전송
의료기기	인슐린 펌프 조작 해킹, 치명적 복용량 주입
IoT 제조사	불법복제, 유통으로 매출 저하 및 회사 이미지 실추
인명사고 유발	오작동, 악의적 조작으로 신체적/정신적 피해 유발, 법적 책임 문제 발생 및 회사 이미지 실추
디바이스, 게이트웨이, 플랫폼, 응용 서비스	Worm, Virus, 기밀성/무결성 공격, 비인가된 접근, 비인가된 I/O 접근, 설정 오류 및 실수, 복제 공격, 보호되지 않는 펌웨어
통신/네트워크	DoS, DDoS의 경유지로 악용, 방화벽의 부적절한 사용, 프로토콜 보안 취약성
플랫폼, 응용 서비스	패치안된 시스템 OS, OS 보안 취약성, Anti-Virus SW의 무분별한 사용, 부적절한 시스템 Log 기록, 프라이버시 침해
응용 서비스 무단이용	비인가된 서비스 접근, 비인가된 사용자의 접근, 안전하지 않은 패스워드 사용, 서비스 인프라 구축 및 운용 비용 증가

〈자료〉 김학용, "사물인터넷 보안 사례 및 대응 방안", 한국인터넷진흥원, 2016.

Stuxnet 공격 등이 있다. IoT 분야별 보안 위협 시나리오는 [표 2]와 같다[2],[3],[6].

III. 5G에서의 차세대 IoT 보안

IoT 공격명과 내용은 [표 3]과 같다[6].

[표 3] IoT 공격명과 내용

공격명	내용
간섭/방해/충돌	노이즈 발생/동시 동일 주파수 접속/주파수 위변조 등을 통해 실제 신호의 정상적인 송수신 방해
시빌(Sybil)	기존의 Wireless Ad-hoc이나 Identity가 허용되는 취약점을 이용한 공격으로, 각 디바이스나 센서에 Unique ID를 부여하지 않을 경우에 발생
교통(Traffic) 분석	암호화되지 않은 NPDU(패킷), DLPDU(프레임) 페이로드를 분석하여 공격
도스(DoS)	주변 노드에 지속적으로 광고 패킷 송신, DLPDU 반복 전송, CRC 반복 체크로 시스템에 부하 가중, 주파수 Jamming으로 송수신 방해
비동기화	디바이스 풀에 잘못된 시간정보를 송신하여 교정시간 소모 유발
벌레구멍(Womhole)	상호통신이 허용되지 않는 두 디바이스의 무선통신 모듈을 공격하고 통신 라우팅을 고의로 변경하여 악성코드 배포경로로 악용
탬퍼링	단말 데이터 송수신 데이터를 임의로 위변조
도청	암호화되지 않은 디바이스(센서)와 게이트웨이 간 정보 도청
선택적 전달 공격	특정 노드에 패킷을 블로킹하여 해당 노드를 블랙홀(Blackhole)화함
스푸핑	공유 키를 취득하여 인가되지 않은 fake 디바이스(센서)를 네트워크에 접속시킴
전파 간섭을 이용한 오작동	ISM(Industrial Scientific Medical band) 대역과 같은 비면허 대역에 과도한 출력 신호 및 과도한 트래픽 발생
데이터 패턴 분석 결과 악용	실시간 감시나 보안관련 사고 유발
배터리 소모를 통한 동작 정지	과도한 패킷 전송이나 프로세싱 유도
디바이스 제어권 탈취	물리적 사고 유발

〈자료〉 김학용, "사물인터넷 보안 사례 및 대응 방안", 한국인터넷진흥원, 2016.

적외선 레이저에 의한 약물 주입기 센서 해킹 및 오작동 유발, 무선에 의한 카드 정보 탈취 및 불법 결제, 네트워크 내 다른 디바이스에 대한 악성 코드 침투 공격, DDoS 공격, 디바이스 배터리 소모, 네스트 온도조절기 해킹, 랜섬웨어 공격, 전광판 제어장치의 접속권한 탈취(미국 텍사스 오스틴), 여수 버스정류소 안내시스템 해킹에 의한 음란 동영상 70분간 노출, 초인종 해킹을 통한 장비 공격(PenTest Partners사), 커넥티드카의 해킹을

통한 원격 제어(체로키의 유커넥티 시스템 해킹), 아마존 판매 CCTV에 대한 악성코드 탑재(DDoS 봇넷에 악용 가능한 코드가 발견), 보안 전문업체 Sucuri에 의해 발견된 2만 5,000대의 CCTV로 구성된 봇넷, Mirai DDoS 봇넷에 의한 Dyn DNS 해킹(2016.5.), 스마트홈 플랫폼인 SmartThings의 해킹(2016.5.) 등 IoT 보안 사고의 발생은 공격 대상의 숫자가 기하급수적으로 증가함으로써 디바이스에 대한 정보 획득이 용이해졌고 기기들의 보안 기능 미탑재와 함께 IoT 보안 공격 시나리오가 많다는 점과 낮은 보안에 대한 인식 등으로부터 기인한다[4],[5],[29].

PC나 모바일 기기가 고전력, 고성능 환경에서 보안 환경을 제공할 수 있었던 반면에 IoT 기기는 저전력, 저성능의 자원으로 보안 기능까지 구현해야하므로, 설계 단계부터 보안성을 고려한 "보안 내재화"가 필수적이며 보안 시스템을 기본적으로 탑재한 제품 제작 및 서비스 설계를 통해 위협을 원천 차단하는 것이 요구된다. 2016년 6월 정부는 "IoT 보안 얼라이언스"를 출범하여 IoT 보안 내재화를 위한 보안 가이드를 발표하였고 이를 통해 IoT 보안 위협에 대응하고 있다[17],[18]. 의료부분과 식약처 및 한국인터넷진흥원은 IoT 공통보안 원칙, IoT 공통보안 가이드, 홈 가전 IoT 보안가이드 등을 제시하고 있다[19],[26]. 여기서 수립한 IoT 공통보안 7대 원칙은 [표 4]와 같다[21].

[표 4] IoT 공통보안 7대 원칙

원칙	내용
1	정보보호와 프라이버시 강화를 고려한 IoT 제품/서비스 설계 - "Security by Design" 및 "Privacy by Design" 기본 원칙 준수
2	안전한 SW, HW 개발 기술 적용 및 검증 - 시큐어 코딩, 소프트웨어, 애플리케이션 보안성 검증 및 시큐어 하드웨어 장치 활용
3	안전한 초기 보안 설정 방안 제공 - "Secure by Default" 기본 원칙 준수
4	보안 프로토콜 준수 및 안전한 파라미터 설정 - 통신 및 플랫폼에서 검증된 보안 프로토콜 사용(암호/인증/인가 기술)
5	IoT 제품/서비스의 취약점 보안 패치 및 업데이트 지속 이행 - S/W와 H/W의 보안 취약점에 대해 모니터링하고 업데이트 지속 수행
6	안전한 운영/관리를 위한 정보보호 및 프라이버시 관리 체계 마련 - 사용자 정보 취득-사용-폐기의 전주기 정보의 보호 및 프라이버시 관리
7	IoT 침해 사고 대응체계 및 책임 추적성 확보 방안 마련 - 보안 사고에 대비한 침입탐지와 사고 시 분석 및 책임 추적성 확보

〈자료〉 미래창조과학부, "사물인터넷(IOT) 정보보호 로드맵", 2014.

많은 수의 IoT 디바이스가 악성 트래픽을 발생시키고 있다. 이것은 아주 오래된 Open SSH(OpenBSD Secure Shell) 취약점을 이용한 해킹으로 IoT 디바이스 약 200만 대 이상의 피해가 예상된다[28]. 공용 네트워크에 존재하는 IoT 디바이스들인 CCTV, NVR, DVR 디바이스, 위성안테나 디바이스, 네트워크 디바이스(라우터, 케이블 컨트롤러, ADSL 모뎀 등)들이 악용되는데, 이는 대부분의 디바이스들이 CVE-2004-1653 취약점 패치를 제대로 진행하지 않았기 때문이다. 이에 대한 예방법으로, 사용자는 IoT에 설정되어 있는 디폴트 계정정보를 수정해야 한다. SSH 통신이 필요한 서비스는 반드시 SSH 서비스를 비활성화시키거나 혹은 AllowTcpForwarding No를 sshd_config내로 이동시킨다. 또한, 방화벽 룰을 추가하여 공격자 IP가 SSH 서비스에 접속하는 것을 차단한다. IoT 제작업체는 로그인 자격증명이 설정되어 있지 않은 IoT 디바이스는 인터넷에 접속하지 못하도록 설정한다. 기본적으로 SSH 서비스가 비활성화되도록 제작하고 SSH 서비스가 TCP 포트를 통해 전달되지 못하도록 제작해야 한다. sshd를 업데이트하여 SSH 취약점을 패치해야 한다[27]. 분야별 보안 취약점은 [표 5]와 같다.

[표 5] 분야별 보안 취약점

분야	내용
스마트 홈, 가전	- 냉장고, TV 해킹으로 스팸메일 발송(proofpoint, 2014. 1.) - 필립스의 LED 전구 제어시스템 해킹 시연(Chanjani, 2013. 8.) - 리눅스 탑재 PC, 가정용 라우터, 셋톱박스, CCTV 등 다양한 디바이스를 감염시킬 수 있는 신규 리눅스 취약점 발견(2013. 11.) - 러시아, 중국산 다리미, 주전자에서 무선인터넷 접속 및 도청 가능한 칩셋 발견(2013. 10.)
스마트카, 교통	- 악성 앱에 감염된 스마트폰을 차량 전자제어장치(ECU)와 연결하여 원격제어 시연(2013. 9.)
스마트 의료	- 심박기에 내장된 전송기(transmitter)의 펌웨어를 해킹하여 전기공급량을 원격 제어하는 해킹 시연(Breakpoint Security Conference, 2012. 10.) - 인슐린 농도를 조절하는 인슐린 펌프의 통신 주파수를 해킹하여 투여량을 조작하는 해킹 시연(BlackHat USA, 2013. 7.)
스마트 그리드	- 푸에르토리코 스마트미터 전직 직원들이 소프트웨어를 불법 조작하여 요금을 2년간 3,400만 달러 미부과 - 미국 일리노이주의 수력발전소 SCADA 시스템이 감염되어 펌프 오동작으로 발전설비 셧다운 발생(2010. 7.)
보안	- 미국 TRENDNet사의 IP카메라 20여 종에서 IP 주소만 알면 누구나 도감청 가능한 소프트웨어 결함 발견(2012. 2.)

〈자료〉 12-Year-Old SSH Bug Exposes More Than 2 Million IoT Devices, 2014.

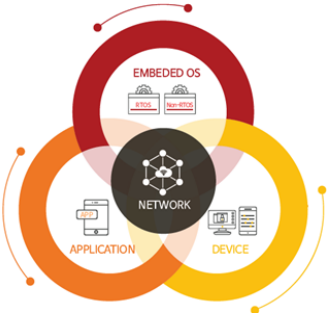
보안전문업체인 이스트시큐리티가 제안하는 IoT 취약점 예방 수칙은 [표 6]과 같다.

[표 6] IoT 취약점 예방 수칙

분야	내용
패스워드 설정	대부분의 IoT 디바이스 사용자는 관리자 혹은 접속 가능한 계정의 패스워드를 출고 당시 기본 패스워드 그대로 사용하거나, 안전하지 않은 패스워드를 사용하는 등 패스워드 설정 미흡으로 정보 유출이 일어난다. 그러므로 초기 패스워드를 주기적으로 변경하고 추측이 어려운 비밀번호를 설정하여 비인가된 사용자의 접근을 방지해야 한다.
암호화 설정	IoT 디바이스 통신에 암호화를 이용하지 않거나, 취약한 암호 방식을 사용할 경우, 공격자는 암호 알고리즘의 취약점을 이용하여 디바이스에 접근하여 사용자의 영상 정보와 같은 특정 정보를 탈취할 수 있다. 이와 같은 보안 위협을 방지하기 위해서 IoT 디바이스 간 송/수신하는 데이터의 암호화가 필요하다. 때문에 안전성을 보장하는 보안 통신 프토로콜인 HPPTS(SSL/TLS 등) 기반 보안 설정이 가능한 제품 이용을 권장하며, IoT 기기를 통해 수집된 개인정보 전송 시 보안 프로토콜을 적용하여 전송하는지 확인해야 한다.
접근제어 설정 IP/MAC 주소 인증	보안 위협을 방지하기 위해 인가된 사용자인지를 확인하고, 비인가자의 보안 위협에 대응할 수 있도록 ID, 패스워드 외에 IP나 MAC 주소 필터링 등의 다양한 인증 수단을 이용하는 IoT 디바이스인지를 체크한다.
펌웨어 업데이트	알려진 취약점으로 인한 악성코드 감염, 정보 유출 등을 방지하기 위해서 제조사에서 알려진 취약점을 해결한 버전을 배포하였는지 보안 공지 내용을 정기적으로 확인하는 등 펌웨어를 늘 최신 버전으로 유지한다.
IoT 보안 취약점 집중 신고기간	한국인터넷진흥원(KISA)이 운영하는 IoT 침해사고 예방을 위한 버그바운티(신고포상제)의 일환으로, 실생활에서 사용되는 IoT 디바이스에 영향을 줄 수 있는 신규 보안 취약점을 신고하여 해결조치를 요청할 수도 있으며, 일부의 경우 신고 포상금도 받을 수 있다.

〈자료〉 보안 위협에 노출된 우리의 일상, IoT 취약점을 아시나요?, EST Seurity 알약 블로그, 2018.

SK인포섹의 IoT 보안 가이드 라인에 따르면 IoT 보안을 크게 [그림 2]의 디바이스, OS, 네트워크, 애플리케이션 4개 영역으로 분류하여 영역별로 각각의 대응방안을 마련하고 있다[24],[25],[28]. OWASP(Open Web Application Security Project), SANS(Sysadmin, Audit, Network, Security), 한국인터넷진흥원이 권고하는 보안 요건을 기반으로 SK인포섹에서 정의한 디바이스, OS, 네트워크, 애플리케이션 영역별 세부 진단 항목은 [표 7]과 같다[22].



〈자료〉 EQST insight, "사물인터넷(IoT) 보안 가이드라인", 2018

[그림 2] IoT 4개 영역

IoT 제품·서비스의 보안문제로 여러 유형의 IoT 보안 가이드들이 제시되고 있다. 기존의 단편적인 이슈 및 대책을 제시하던 것에 비해 2016년에는 일본 정보처리기구 IPA(Information-technology Promotion Agency), 국제이동통신사업자협회인 GSMA(Global System for Mobile communication Association), 국제 웹보안표준단체인 OWASP(The Open Web

[표 7] 영역별 세부 진단 항목

영역	분류	세부 진단 황목	
디바이스	권한	취약한 보안 설정	불필요한 포트/서비스 오픈: 취약한 BIOS 설정
		접근제어	취약한 물리적 인터페이스 접근제어
	인증	인증관리	등록, 초기화, 분식 액세스 절차 검증
		계정관리	취약한 계정관리
	기밀성	통신구간 보호	요청 및 응답 데이터 내 중요 정보 노출 여부
		메모리 보호	메모리 내 중요 정보 노출 여부: 메모리 내 암호화 키/함수 보유
	무결성	펌웨어 보호	펌웨어 무결성 검증: 펌웨어 변조 가능 여부
		디바이스 보호	디바이스 개조 가능 여부
	기타	기타 취약점	취약한 진단 항목에 정의되지 않은 취약점
OS	권한	취약한 보안 설정	부트로더 조작 가능 여부
		접근제어	TPM(Trusted Platform Module) 설정 여부 확인: 관리자/CLI 접근제어 설정 여부 확인
	인증	인증관리	인증정보 위조 도용 가능성 여부 확인: 등록/초기화/분실 액세스 절차 검증

〈자료〉 Internet & Security Bimonthly, "사물인터넷 보안 위협 동향", Vol.5, 2014.

Application Security Project), 국제 클라우드 보안 협의체인 CSA(Cloud Security Alliance) 등에서 IoT 기기의 보안 설계·개발 및 안전한 서비스 운영 등을 위한 보안 요구사항과 대책을 포함한 상이한 유형의 보안 가이드를 발표하였다. 국내외에 현재까지 발표된 IoT 관련 보안가이드는 [표 8]과 같다[22].

[표 8] 국외 IoT 보안 가이드

기관	보안 가이드
GSMA	서비스 생태계, 엔드 포인트 생태계, 네트워크 운영자를 위한 IoT 보안 가이드(2016년 12월)
IPA	연결 세계 개발 지침(2016년 3월): IoT 개발의 보안설계 가이드(2016년 5월)
OWASP	IoT 보안지침 초안(2016년 5월)
OTA	IoT 신뢰 프레임워크(2016년 7월)
CSA	사물인터넷의 초기 채택자를 위한 보안 지침(2015년 4월)

〈자료〉 Internet & Security Bimonthly, "사물인터넷 보안 위협 동향", Vol.5, 2014.

GSMA는 세계 모바일 사업자의 이익을 대표하며, 광의의 모바일 생태계에 속한 250여 개 업체를 포함하여 800개에 육박하는 모바일 사업자를 하나로 묶고 있다. 단말기 및 기기 제조사, 소프트웨어 기업, 장비 공급사, 인터넷 기업은 물론 인접 산업 분야 기관들이

함께 하며 모바일 월드 콩그레스, 모바일 월드 콩그레스 상하이, 모바일 360 시리즈 컨퍼런스 등 업계 선도적인 행사를 주최하고 있다. 2018년 6월 27일 AT&T, 차이나 모바일(China Mobile), 차이나 텔레콤(China Telecom), 차이나 유니콤(China Unicom), 도이치 텔레콤(Deutsche Telekom), 에티살랏(Etisalat), KDDI, LG유플러스, 오렌지(Orange), 텔레포니카(Telefonica), 텔레노어 그룹(Telenor Group), 텔리아(Telia), 투르크셀(Turkcell), 보다폰 그룹(Vodafone Group), 자인 그룹(Zain Group) 등 글로벌 모바일 사업자들이 GSMA IoT 보안 가이드라인을 채택, 실행할 것이라고 발표했다[16].

이 가이드라인은 IoT 생태계의 IoT 서비스가 보안 리스크에 충분한 보안장치가 되어 있는지를 확인하는 종합적인 보안평가 시스템을 설명한다. LG유플러스는 2018년 GSMA IoT 보안 챔피언을 수상하기도 하였다. 모바일 업계는 정부 제공 주파수 대역폭 하에서 높은 보안성의 서비스를 제공해온 자랑스런 역사를 갖고 있으며 이번 가이드라인을 실행함으로써 앞으로도 계속해서 지속 가능한 성장을 할 수 있도록 만전을 기하고 있다고 말했다. GSMA의 IoT 보안 가이드라인은 IoT 서비스 제공업체, 기기 제조업체, 개발회사, 모바일 사업자 등을 대상으로 하며, 업계 전체에 걸쳐 높은 보안성의 IoT 솔루션 디자인과 개발, 설치 등을 위한 최근 사례를 제공하고 있다[6]. 이 가이드라인에서는 IoT 서비스와 관련된 통상의 사이버 보안과 데이터 프라이버시 문제도 언급하고 있고 IoT 솔루션의 출시를 지원하는 체크리스트를 제공하고 서비스 전역에 걸쳐 높은 보안을 유지해주는 IoT 생태계를 만든다는 목표를 지향하는 IoT 보안 평가 제도(IoT Security Assessment scheme)를 통해서 지원을 받고 있다. GSMA의 IoT 보안 가이드라인과 IoT 보안 평가는 모두 급속한 성장을 거듭하는 LPWA 및 LTE-M과 NB-IoT를 포함하는 모바일 IoT 기술을 대상으로 하고 있다.

보안가이드를 개발하는 기관 및 단체의 특성에 따라 보안 취약점, IoT 기기의 생명주기, IoT 서비스의 구성요소(단말, 네트워크, 서비스) 등 서로 다른 기준에서 각기 다른 관점으로 보안가이드를 제시하고 있음에도 불구하고 IoT를 구성하는 단말과 네트워크, 서비스 등에 대해서는 일반적인 보안 요구사항을 다수 포함하고 있고 가이드 내용은 대부분 유사하다. 그리고 현재까지 공개된 국외 IoT 관련 보안가이드는 대부분 초기버전에 해당되며 IoT 서비스가 산업 분야별로 다양함에 따른 보안 요구사항에 대한 대책으로 특정 기술이나 상세한 보안대책을 제시하지는 못하고 있다. 이로 인해 IoT 관련 국외 보안가이드에서

는 현재 상태에서의 IoT 기술 및 현황을 바탕으로 일반적인 보안대책을 제시하고 있으며, 이후 IoT 기술 개발 및 발전방향에 따라 IoT 관련 보안가이드의 내용은 추후 업데이트가 진행될 것으로 보인다. 2015년 6월 발족한 국내 최대 민간 사물인터넷 보안 협의체인 IoT보안얼라이언스에서 제시하는 IoT 보안 공통 가이드는 [표 9]와 같다[17].

IoT 보안 요구사항에 따른 보안 가이드를 기준으로 IoT 디바이스에 대한 보안 점검 기준은 [표 10]과 같다.

[표 9] IoT 보안 공통 가이드

단계	IoT 공통 보안 원칙	IoT 공통 보안 가이드
설계 개발	정보보호와 프라이버시를 고려한 IoT 제품·서비스 설계	① IoT 장비 특성을 고려하여 보안 서비스의 경량화 구현 ② IoT 서비스 운영 환경에 적합한 접근권한 관리 및 인증, 종단 간 통신 보안, 데이터 암호화 등의 방안 제공 ③ 소프트웨어 기술 보안과 하드웨어 보안 기술의 적용 검토 및 안전성이 검증된 보안 기술 활용 ④ IoT 제품 및 서비스에서 수집되는 민감 정보(개인정보 등) 보호를 위해 암호화, 비식별화, 접근관리 등의 방안 제공 ⑤ IoT 서비스 제공자는 수집하는 민감 정보의 이용목적 및 기간 등을 포함한 운영정책 가시화 및 사용자에 투명성 보장
	안전한 SW 및 HW 개발기술 적용 및 검증	⑥ 소스코드 구현단계부터 내재될 수 있는 보안 취약점을 사전에 예방하기 위해 시큐어 코딩 적용 ⑦ IoT 제품 및 서비스 개발에 사용된 다양한 SW에 대해 보안 취약점 점검 수행 및 보안 패치 방안 구현 ⑧ 펌웨어/코드 암호화, 실행코드 영역제어, 역공학 방지 기법 등 다양한 하드웨어 보안 기법 적용
배포 설치 구성	안전한 초기 보안 설정 방안 제공	⑨ IoT 제품 및 서비스 (재)설치 시 보안 프로토콜들에 기본으로 설정되는 파라메터값이 가장 안전한 설정이 될 수 있도록 “Secure by Defalut” 기본 원칙 준수
	안전한 설치를 위한 보안 프로토콜 준수 및 안전한 파라메터 설정	⑩ 안전성을 보장하는 보안 프로토콜 적용 및 보안 서비스 제공 시 안전한 파라메터 설정
운영 관리 폐기	IoT 제품·서비스 취약점 패치 및 업데이트 지속 이행	⑪ IoT 제품 및 서비스의 보안 취약점 발견 시 이에 대한 분석 수행 및 보안 패치 배포 등의 사후조치 방안 마련 ⑫ IoT 제품 및 서비스에 대한 보안 취약점 및 보호조치 사항은 홈페이지, SNS 등을 통해 사용자에게 공개
	안전 운영·관리를 위한 정보보호 및 프라이버시 관리체계 마련	⑬ 최소한의 개인정보만 수집·활용될 수 있도록 개인정보보호정책 수립 및 특정 개인을 식별할 수 잇는 정보의 생성·유통을 통제할 수 있는 기술적·관리적 보호조치 포함
	IoT 침해사고 대응체계 및 책임 추적성 혹보 방안 마련	⑭ 다양한 유형의 IoT 장치, 유·무선 네트워크, 플랫폼 등 다양한 계층에서 발생 가능한 보안 침해사고에 대비하여 침입탐지 및 모니터링 수행 ⑮ 침해사고 발생 이후 원인분석 및 책임 추적성 확보를 위해 로그기록의 주기적 저장·관리

〈자료〉 한국인터넷진흥원, “IoT 공통 보안 가이드”, 2016.

[표 10] IoT 디바이스 보안 점검 기준

방안	보안 점검 항목 및 기준
접근권한 관리 및 인증	접근 계정 및 권한 확인 - 유지보수 목적으로 제조사 등에서 접속하는 관리자 계정 사용 중지 - 인증된 클라이언트는 타 클라이언트의 데이터에 접근하지 못하도록 권한 관리
	개인정보 수집 시 개인정보보호 관리체계 수립 후 기술적, 관리적 보호조치 수행
	수집된 개인(민감)정보의 접근관리, 인증, 저장 및 전송 시 암호화 등 보호조치 필요
	비밀번호 정책 - 관리자 계정의 모든 디바이스에 공통 비밀번호 사용 금지 - 펌웨어 등 디바이스에 비밀번호 저장 금지 - 특정 횟수 이상 비밀번호가 틀리는 경우 계속 시도하지 못하도록 재시도 딜레이 추가
종단간 통신 보안 및 데이터 암호화	알고리즘 및 적정한 키 길이에 따른 안전성 확인
	통신구간 암호화는 전구간 TLS 적용 권장
	Salt, iv 사용으로 암호화 안전성 확보
	암복호화용 키는 소스코드나 시스템 내부 파일 형태로 저장 금지
	안전한 키 관리를 위해서는 하드웨어 기반 보안 솔루션 사용 권장
보안 적용 기술 방식 확인	적용기술의 안전성 확인 - 적용된 보안 기술 목록 및 안전성 검토 결과 요청 - 암호모듈 검증 또는 CC 인증 여부 확인
	하드웨어 보안 기법 적용 - 디버깅용 입출력 포트(UART/JTAG 등) 이용 디바이스 내부 shell 연결 및 실행 기능 - IoT 서비스의 특성상 고도의 보안 요구 시 시큐어 부트, 펌웨어 코드/암호화, 실행 코드 영역 제어 등 하드웨어 보안 기법 적용 필요
시큐어 코딩 및 보안 패치	시큐어 코딩 적용 여부 확인 - 소스코드 취약점 제거를 위한 시큐어 코딩 적용 여부 확인 - 패치버전의 시큐어 코딩 적용 여부 확인
	지속적인 보안 취약점 점검 및 패치방안 - 보안 취약점 점검 주기 및 일정 확인 - 안전한 보안 패치 적용 방안

〈자료〉 한국인터넷진흥원, "IoT 공통 보안 가이드", 2016.

IV. 결론

이미 생활 속에 깊이 자리잡고 있는 IoT에 대해 보안을 개인이 알아서 대처하라는 것은 현실적으로 상당히 어려운 부분이 있다. 따라서 IoT 보안과 관련하여 정부와 정부부처에서는 지속적으로 5G 보안 정책을 제시하고 관련 법규를 제정해야 할 것이며, 학회나 협회,

포럼 등에서는 5G 보안 표준을 제안하고 핵심 원천기술 표준을 선점하고 미래 지적재산권(Intellectual property rights)을 확보해야 한다. 또한, 학계에서는 5G 보안 분석 및 검증과 차세대 보안 기술 연구가 요구되며, 보안 업체나 제조사, 통신사들은 언론기관과 산업계, CP(Contents Provider), 보안인증/심사기관과 협업하여 안전한 5G 네트워크 환경 구축과 국민 편익 중심의 융합 서비스 제공에 힘써야 하며, 정보공유분석센터(Information Sharing & Analysis Center)나 컴퓨터 침해사고 대응반(Computer Emergency Response Team)과 협업을 해야 할 것이다.

IoT 제품이나 서비스에 상존하는 보안 위협은 잘 정의된 아키텍처와 보안관련 사건 전후에 위험을 찾아내는 정보력, 그리고 사건을 처리하는 정책과 절차만 잘 정비되어 있다면 거의 모두 대처할 수 있다. IoT 서비스 업체에게 어떤 보안 개념이 중요한지를 문의한다면 가장 시급한 취약점 해결에 도움을 받을 수 있을 것이다. 보안 상의 의문점과 우려사항이 구현 시점에서 드러나서 조직적 관점에서 이를 공유하고 대처 전략을 세우고 여러 사람의 기술과 지식을 데이터베이스로 구축한다면 IoT 보안에 대비할 수 있다. 결론적으로, 정부 및 산/학/연 상호 협업의 플랫폼 허브(Platform HUB)를 통한 5G 보안 생태계 육성이 반드시 필요하다.

[참고문헌]

[1] 강남희, “사물인터넷 보안을 위한 표준기술 동향”, 한국통신학회지(정보와통신) 31.9, 2014, pp.40-45.
[2] 고윤승, “전자무역: 사물인터넷(IoT) 의 주요국 정책과 시장전망에 관한 연구”, 통상정보연구 16.5, 2014, pp.27-47.
[3] 김기환, 김대철, 신용태, “사물 인터넷(IoT) 동향 및 차세대 보안 기술방안 연구”, 한국인터넷정보학회 학술발표대회 논문집, 2015, pp.69-70.
[4] 김동희, 윤석웅, 이용필, “IoT 서비스를 위한 보안”, 한국통신학회지(정보와통신) 30.8, 2013, pp.53-59.
[5] 김우년, “Homeland Security에서의 M2M(사물지능통신) 보안 동향”, 정보보호학회지, 제22권 제2호, 2, 2012.
[6] 김학용, “사물인터넷 보안 사례 및 대응 방안”, 한국인터넷진흥원, 11, 2016.
[7] 김해용, 지장현, 김호원, “안전한 IoT 서비스를 위한 디바이스 보안과 플랫폼 보안 연동”, 정보보호학회지 28.5, 2018, pp.26-30.
[8] 김호원, “사물인터넷 환경에서의 보안/프라이버시 이슈”, TTA Journal Vol.153, 2014. 5. 6.
[9] 김호원, “사물인터넷 서비스에서의 보안 이슈”, 정보과학회지 32.6, 2014, pp.37-41.
[10] 서화정, 이동건, 최종석, 김호원, “IoT 보안 기술 동향”, 전자파기술 24.4, 2013, pp.27-35.
[11] 손태식, 고종빈, “Cloud Computing에서의 IOT(Internet of Things) 보안 동향”, 정보보호학회지,

제22권 제2호, 2, 2012.
[12] 이미승, 김태성. “사물인터넷기기의 보안위협에 대한 연구: 핏빗(Fitbit) 사례”, 대한경영학회 학술대회, 2018, 20-20.
[13] 정용식, 차재상, “IoT 디바이스 보안 점검 기준”, 한국통신학회지(정보와통신) 34.2, 2017, pp.27-33.
[14] 미래창조과학부, “사물인터넷(IOT) 정보보호 로드맵”, 2014. 10.
[15] 이스트시큐리티, “보안 위협에 노출된 우리의 일상, IoT 취약점을 아시나요?”, 2018. 2.
[16] EQST insight, “사물인터넷(IoT) 보안 가이드라인”, 2018. 9.
[17] 식약처, “의료기기 사이버보안 가이드라인”, 2018. 1.
[18] Internet & Security Bimonthly, “사물인터넷 보안 위협 동향”, Vol.5, 2014.
[19] “사물인터넷 시대의 안전망, 융합보안산업”, Cisco, Gartner, Machine Reserach, K&C Consurting 산업연구원, 2014. 4.
[20] 한국인터넷진흥원, “홈·가전 IoT 보안가이드”, 2017. 7.
[21] SSHowDowN, AKAMI THREAT ADVISORY, 2016. 10.
[22] GSMA, “IoT 서비스 생태계를 위한 IoT 보안 지침”, 2017.
[23] 한국인터넷진흥원, “IoT 공통 보안 가이드”, 2016.
[24] 한국인터넷진흥원, “IoT 공통 보안 원칙 v1.0”, 2016.
[25] Matk Weisr, “The Computer for 21st Century”, Scientific American, 1991.
[26] OWASP Internet of Things Top Ten, 2018
[27] 12-Year-Old SSH Bug Exposes More Than 2 Million IoT Devices, 29, 2014. 10.
[28] 정보화진흥원, “5G가 만들 새로운 세상 보고서”, 2019. 3.